IEEE P802.11
Wireless LANs

|  |
| --- |
| New Test Vectors for SAE |
| Date: 2018-06-25 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE | 3333 Scott BoulevardSanta Clara, California, United States of America |  |  |
|  |  |  |  |  |

Abstract

This submission updates the test vectors for SAE.

***Instruct editor to replace J.10 SAE Test Vector with the following:***

**group:** 19

**password:** mekmitasdigoat

**password identifier:** psk4internet

**local MAC address:** 82:7b:91:9d:d4:b9

**peer's MAC address:** 1e:ec:49:ea:64:88

**H(82:7b:91:9d:d4:b9 || 1e:ec:49:ea:64:88, mekmitasdigoat || psk4internet || 1)**

b39919ad 439eee7d b61d9564 421700ac b9ed1044 577ce934 5e38c97d e673c3f0

**candidate x value:**

282167aa 6ba380c5 3a9c5230 c0b53b1e bc456983 cc05f0f2 b869a75f 7f232e91

**PWE (x,y):**

282167aa 6ba380c5 3a9c5230 c0b53b1e bc456983 cc05f0f2 b869a75f 7f232e91

cc8a5450 65e3a76c 6731a0f4 471a3384 42ef3cc3 c978e787 e0d5cdc9 07dd4e9c

**local private value:**

a906f61e 4d3a5d4e b2965ff3 4cf917dd 044445c8 78c17ca5 d5b93786 da9f83cf

**local mask value:**

4234b4fb 17aa435c 52fbfdeb e64039b4 3478200e 54ff7b6e 07b69cad 74153c15

**local commit:**

1300eb3b ab1964e4 a0ab0592 5ddf3339 519138bc 65d6cdc0 f813dd6f d4344eb4

bfe44b5c 21597658 f4e3eddf b4b99f25 b4d6540f 32ff1fd5 c530c60a 79444861

0bc6de3d 92bdbbd4 7d935980 ca6cf898 8ab6630b e6764c88 5ceb9793 970f6952

17eeff0d 2170736b 34696e74 65726e65 74

**peer private value:**

a47d07bb d3d1b618 b325dfde 02413a45 0a90fd1e e1ac35f4 d3856cc9 cb77128c

**peer mask value:**

b0e7e888 df18683e b9cbfd96 1d2f9f78 e828dcea 5fc06b24 8f149af2 0bce90e3

**peer commit:**

13005564 f045b2ea 1e566cf1 dd741f70 d9be35d2 df5b9a55 02946ee0 3cf8dae2

7e1e05b8 430eb7a9 9e24877c e69baf3d c580e309 633d6b38 5f83ee1c 3ec3591f

1a5393c0 6e805ddc eb2fde50 930dd7cf ebb987c6 ff9666af 164eb518 4d8e6662

ed6aff0d 2170736b 34696e74 65726e65 74

**k:**

ad68ea33 9d3db924 f4ccee64 bcc0609e d8258760 dd85428b b3194f26 2dff4888

**keyseed:**

7457a007 54dcc4e3 dc2850c1 24d6bb8f a1699d7f a33bb066 7d9c34ee b513deb9

**KCK:**

599d6f1e 27548be8 499dceed 2feccf94 818ce1c7 9f1b4eb3 d6a53228 a09bf3ed

**local confirm:**

010012d9 d5c78c50 0526d36c 41dbc56a edf2914c edddd7ca d4a58c48 f83dbde9

fc77

**peer's confirm:**

01000287 1cf90689 8b8060ec 184143be 77b8c08a 8019b13e b6d0aef0 d8383dfa

c2fd

**PMK:**

7aead86f ba4c3221 fc437f5f 14d70d85 4ea5d5aa c1690116 793081ed a4d557c5

**PMKID:**

40a09b60 17cebf00 72843b53 52aa2b4f

**References:**